

## Release Notes

# LCOS 10.72 SU2

### Inhaltsübersicht

02	<b>1. Einleitung</b>
02	<b>2. Das Release-Tag in der Software-Bezeichnung</b>
03	<b>3. Gerätespezifische Kompatibilität zu LCOS 10.72</b>
03	<b>4. Hinweise zu LCOS 10.72</b>
03	Informationen zu Werkseinstellungen
04	<b>5. Feature-Übersicht LCOS 10.72</b>
04	<b>5.1 Feature-Highlights 10.72</b>
04	Advanced Mesh VPN
04	<b>5.2 Weitere Features LCOS 10.72</b>
04	Jugendschutz nach BPjM-Vorgaben
04	Zwei-Faktor-Authentifizierung – Doppelte Sicherheit für Ihr VPN
06	<b>6. Historie LCOS 10.72</b>
06	LCOS-Änderungen 10.72.0092 SU2
07	LCOS-Änderungen 10.72.0091 RU1
10	LCOS-Änderungen 10.72.0015 Rel
12	<b>7. Allgemeine Hinweise</b>
12	Haftungsausschluss
12	Sichern der aktuellen Konfiguration
12	Verwendung einer Minimalfirmware zur Vergrößerung des Speicherplatzes

## 1. Einleitung

Alle Mitglieder der LANCOM Betriebssystem-Familie – LCOS, LCOS SX, LCOS LX und LCOS FX – sind die vertrauenswürdige Grundlage für das gesamte LANCOM Produktportfolio. Im Rahmen der von den Produkten vorgegebenen Hardware ist die jeweils aktuelle Firmware-Version für alle LANCOM Produkte verfügbar und wird von LANCOM Systems kostenlos zum Download angeboten.

Dieses Dokument beschreibt die Neuerungen der LCOS Software Release 10.72 SU2 sowie die Änderungen und Verbesserungen zur Vorversion.

**Beachten Sie vor der Durchführung des Firmware-Update unbedingt die Hinweise im Kapitel 7 „Allgemeine Hinweise“ dieses Dokumentes.**

Aktuelle Support-Hinweise und sowie Informationen über bekannte Einschränkungen zur aktuellen LCOS-Version finden Sie im Support-Bereich unserer Webseite [www.lancom.de/service-support/soforthilfe/aktuelle-support-hinweise](http://www.lancom.de/service-support/soforthilfe/aktuelle-support-hinweise)

## 2. Das Release-Tag in der Software-Bezeichnung

### **Release Candidate (RC)**

Ein Release Candidate ist umfangreich von LANCOM getestet und enthält neue Betriebssystem-Features. Er dient als Praxistest und wird deshalb für den Einsatz in Produktivumgebungen nicht empfohlen.

### **Release-Version (Rel)**

Das Release ist umfangreich geprüft und in der Praxis erfolgreich getestet. Es enthält neue Features und Verbesserungen bisheriger LANCOM Betriebssystem-Versionen. Wird für den Einsatz in Produktivumgebungen empfohlen.

### **Release Update (RU)**

Dient zur nachträglichen Weiterentwicklung einer initialen Release-Version und enthält Detailverbesserungen, Bug Fixes und kleinere Features.

### **Security Update (SU)**

Enthält wichtige Security Fixes des jeweiligen LANCOM Betriebssystem-Versionstandes und sichert Ihnen fortlaufend einen sehr hohen Sicherheitsstandard.

### 3. Gerätespezifische Kompatibilität zu LCOS 10.72

Grundsätzlich werden alle LANCOM Produkte über die gesamte Lebenszeit regelmäßig mit Major Releases bedient, welche neue Features und Bugfixes beinhalten.

Auch für Geräte, die keine aktuelle LCOS-Version unterstützen, werden in regelmäßigen Abständen LCOS Release Updates inklusive Bugfixes und allgemeinen Verbesserungen bereitgestellt. Eine Übersicht über die aktuell unterstützte LCOS-Version für Ihr Gerät finden Sie unter

[www.lancom.de/produkte/firmware/software-lifecycle-management](http://www.lancom.de/produkte/firmware/software-lifecycle-management)

#### **Die Unterstützung für die folgenden Geräte entfällt ab LCOS 10.72:**

- LANCOM 1781EF+
- LANCOM 1783VA
- LANCOM 1781VAW
- LANCOM 1783VA-4G
- LANCOM R883VAW
- Business LAN R800A

### 4. Hinweise zu LCOS 10.72

#### **Informationen zu Werkseinstellungen**

Geräte, die mit LCOS 10.00 oder größer ausgeliefert werden, kontaktieren automatisch die LANCOM Management Cloud (LMC). Diese Funktionalität ermöglicht eine Zero-Touch-Inbetriebnahme von neuen Geräten. Falls die LMC nicht verwendet werden soll, kann diese Funktionalität über den Grundeinstellungs-Wizard bei der Erstinstallation oder im LANconfig jederzeit unter Management > LMC deaktiviert werden. Eine spätere Verwendung der LMC ist jederzeit wieder manuell aktivierbar.

## 5. Feature-Übersicht LCOS 10.72

### 5.1 Feature-Highlights 10.72

#### **Advanced Mesh VPN**

Bei klassischen, sternförmigen VPN-Standortvernetzungen, in denen alle Filialen lediglich über die Zentrale und nicht direkt untereinander verbunden sind, wird die Internetleitung der Zentrale schnell zum Flaschenhals der gesamten Kommunikation. Mit Advanced Mesh VPN kommunizieren die Zweigstellen nun auf direktem Weg miteinander und sorgen so in der Zentrale für deutlich weniger Traffic und einhergehend für höhere Performance. Die VPN-Tunnel werden hierbei bei Bedarf dynamisch aufgebaut, sobald Datentransfer von einer zur anderen Filiale transportiert wird. Findet keine Kommunikation mehr statt, wird die VPN-Verbindung ebenso dynamisch wieder abgebaut.

### 5.2 Weitere Features LCOS 10.72

#### **Jugendschutz nach BPjM-Vorgaben**

Mit LCOS 10.70 RC1 maximieren Sie jetzt den Schutz von minderjährigen Nutzern z. B. in Schulen oder Jugendeinrichtungen. So ist die offizielle Webseiten-Liste der Bundesprüfstelle für jugendgefährdende Medien (BPjM) nun auch Teil der LANCOM Content Filter Option oder separat über die Software-Erweiterung LANCOM BPjM Filter Option erhältlich (ab LCOS 10.70 Rel). Damit sind Domains, deren Inhalte offiziell als jugendgefährdend eingestuft werden, für die entsprechende Zielgruppe in Deutschland nicht erreichbar. Eine stetige Aktualisierung und Erweiterung dieser Auflistung ist dabei gewährleistet.

#### **Zwei-Faktor-Authentifizierung – Doppelte Sicherheit für Ihr VPN**

Immer dann, wenn ein hohes Sicherheitslevel für Ihre sensiblen Daten erforderlich ist oder z. B. auch Compliance-Richtlinien in Ihrem Unternehmen es vorsehen, ist die doppelte Absicherung des Netzwerk-Zugangs über den LANCOM Advanced VPN Client ideal. Dank Zwei-Faktor-Authentifizierung (IKEv2 EAP-OTP) schützen Sie jetzt den VPN-Zugang und damit auch Ihr Netzwerk vor unbefugten Zugriffen. So kann festgelegt werden, dass sich User ausschließlich über den LANCOM Advanced VPN Client einwählen können, sofern sie beim Login die Zwei-Faktor-Authentifizierung nutzen. Hierbei wird das VPN-Passwort um ein zeitbasiertes Einmalpasswort ergänzt, welches in einer Authentifizierungs-App (z.B. Google Authenticator) auf dem Mobiltelefon generiert werden kann.

Nutzbar ist dieses Feature mit allen Geräten, die mindestens 25 VPN-Tunnel besitzen (entweder bereits integriert oder aber mit LANCOM VPN Option aufgerüstet).

**Weitere Features finden Sie in den Abschnitten zu den einzelnen Builds im Kapitel 6 „Historie LCOS“.**

## 6. Historie LCOS 10.72

### LCOS-Änderungen 10.72.0092 SU2

#### Korrekturen / Anpassungen

##### Allgemein

→ Sicherheitsverbesserungen durch ein Update der OpenSSL-Version auf 1.1.1t (CVE-2023-0286, CVE-2022-4304, CVE-2023-0215 und CVE-2022-4450).

## LCOS-Änderungen 10.72.0091 RU1

### Neue Features

- Beim DHCPv6 Relay Agent können nun bis zu 4 Ziele zur Weiterleitungen an externe Server konfiguriert werden.
- Der DHCPv6 Relay Agent unterstützt eine Absendeadresse in Richtung DHCPv6-Server.
- Das BPJM-Modul besitzt nun eine CLI-Funktion zur Löschung der aktuellen Signaturdefinition.
- „Connection Refused“-Meldungen werden nun im Syslog mit Level ‚Info‘ statt „Alarm“ angezeigt. Dies führt dazu, dass diese Meldungen nicht mehr im Syslog der WEBconfig im Default angezeigt werden. Das Verhalten kann durch eine Konfigurationsänderung angepasst werden.

### Hinweis:

Ab der nächsten LCOS-Major-Version werden die Spalten ‚Tx-normal‘, ‚Tx-reliable‘ und ‚Tx-urgent‘ der Status-Tabelle ‚Status/WAN/Packet-Transport‘ entfernt und nicht mehr unterstützt. Ebenso entfällt dort die Status-Tabelle Status/IP-Router/Protocol-Table. Die letzte unterstützte Version ist LCOS 10.7x.

### Korrekturen / Anpassungen

#### Allgemein

- Das Feature BPJM konnte auch konfiguriert werden, wenn keine Lizenz für diese Option vorhanden war.
- Der WEBconfig-Setup-Assistent zur Einrichtung einer IPv6-Internetverbindung schrieb das Kommentarfeld in die ‚Router‘-Spalte der IPv6-Routing-Tabelle. In der Folge war die konfigurierte IPv6-Verbindung nicht funktionsfähig.
- Wenn zeitweise keine Daten über die 4G- / 5G-Internetverbindung der Deutschen Telekom übertragen wurden, konnte es vorkommen, dass die WWAN-Internetnetverbindung nach Wiederaufnahme der Datenübertragung nicht mehr funktionsfähig war.
- Sobald eine neue Konfiguration per Skript in einen LANCOM 1900EF-5G eingespielt wurde, verblieb das WWAN-Modem im Status ‚Device Removal/ Deactivated‘. Das WWAN-Modem konnte erst durch einen Neustart des Gerätes wieder in den Aktiv-Modus versetzt werden.

- Wenn im Passwort einer verschlüsselten Konfigurationssicherung ein ‚+‘-Zeichen enthalten war, konnte die verschlüsselte Konfigurationsicherung nicht mehr entschlüsselt und in das LANCOM Gerät übertragen werden.
- Bei einem aktiven Backup über WWAN konnte es vorkommen, dass nach einiger Zeit das Routing zwischen LAN und WAN nicht mehr funktionierte und nur durch eine Trennung der WWAN-Verbindung wiederhergestellt werden konnte.
- In Einzelfällen konnte es vorkommen, dass der DHCP-Server auf einem Router im Werkszustand (Einstellung ‚Automatisch‘) nicht startete und dadurch keine IP-Adressen verteilen konnte.
- Empfang der Router einen Broadcast für ein bestimmtes Netzwerk auf dem Interface eines anderen Netzwerks, führte dies zu einem unvermittelten Neustart des Routers, wenn in der Firewall eine Regel mit der empfangenen Broadcast-Adresse als Ziel angelegt war.
- Bei Verwendung von ICMP-Polling für eine Internet-Verbindung kam es zu einem unvermittelten Neustart des Routers, wenn eine ARP-Anfrage des Polling-Ziels beantwortet wurde, bevor die Internet-Verbindung aufgebaut war.
- Wenn bei einer DNS-Anfrage des LMC-Clients mehrere IP-Adressen aufgelöst wurden, verwendete das Gerät für die Kommunikation per TCP immer die ‚kleinste‘ IP-Adresse statt eine Lastverteilung auf mehrere IP-Adressen durchzuführen. Dieses Verhalten betraf auch weitere Anwendungen. Es wird jetzt immer eine zufällige IP-Adresse verwendet.

### VoIP

- Wenn am Router Analog- bzw. ISDN-Geräte angebunden waren, sendete der Voice Call Manager im ‚SDP Answer‘ immer die Codecs PCMA (G.711-a) und PCMU (G.711-u), sobald einer der beiden Codecs im ‚SDP Offer‘ enthalten war. Jetzt werden alle Codecs außer PCMA und PCMU aus dem ‚SDP Offer‘ gelöscht und der erste Codec in die ‚SDP Answer‘ übernommen. Wenn PCMU verwendet wird, transcodiert der Voice Call Manager dies in PCMA, da ISDN- und Analog-Geräte lediglich PCMA unterstützen. Ist im INVITE kein ‚SDP Offer‘ enthalten, antwortet der Voice Call Manager im ‚SDP-Answer‘ mit PCMA und PCMU.
- War in einer SIP-Leitung bei der ‚Signalisierungs-Verschlüsselung‘ die Option ‚Automatisch‘ ausgewählt (NAPTR aktiv), konnte es vorkommen, dass die Re-Registrierung nicht funktionierte und eine Neu-Registrierung durchgeführt werden musste. Dadurch funktionierte in diesem Zeitraum die Telefonie nicht mehr.



- Wird ein Router mit Voice Call Manager vor einer SIP-TK-Ankage eingesetzt, fungiert dieser als Session Border Controller (SBC). Wenn in einem solchen Szenario ein eingehendes Telefonat eines Mobilfunk-Teilnehmers (VoLTE) direkt über die Funktion ‚Verbinden ohne Rückfrage‘ (Blind Call Transfer) weitergeleitet wurde, handelte der Voice Call Manager mit einer bestimmten Gegenstelle des SIP-Providers den Codec nicht korrekt aus. Dies führte dazu, dass das Telefonat abgebaut wurde.
- Verwendete ein SIP-Provider DNS-SRV-Einträge mit der gleichen Priorität, wechselte der Voice Call Manager bei jeder erneuten DNS-Auflösung zwischen diesen Servern. Dies führte zu einer kurzen Unterbrechung der Registrierung.

## LCOS-Änderungen 10.72.0015 Rel

### Neue Features

- Unterstützung von Q-in-Q-VLAN auf WAN-Schnittstellen
- Unterstützung einer Absendeadresse für den Updateprozess der Signaturdatei beim BPJM-Filter
- Master-Holddown-Zeit-Schalter im VRRP
- Unterstützung für RADSEC-Zertifikate im SCEP-Client
- In der WEBConfig gibt es im Dashboard bei WLAN einer Verlinkung zur WLAN-Stationstabelle.
- Ein LANCOM WLC unterstützt die Auswahl des LX-6500 im Firmware-Management.
- Unterstützung von LANCOM ARC 2.0 zusammen mit der LMC

### Korrekturen / Anpassungen

#### Allgemein

- Obwohl auf einem Router keine Content Filter-Option aktiv war, wurde im WEBconfig das Menü ‚Content Filter‘ angezeigt. Die Konfigurationsdialoge waren jedoch leer.
- In der WEBconfig fehlten im Menü ‚Datum/Zeit / Synchronisierung‘ die Konfigurationseinstellungen zur Zeitserver-Abgleichmethode.
- Im WEBconfig-Menü ‚Setup Assistent / Public Spot Benutzer verwalten‘ wurden Benutzer als ‚unauthenticated‘ angezeigt, obwohl diese erfolgreich mit dem Public Spot verbunden waren.
- Bei einer WWAN-Verbindung, bei welcher der Adressbezug per DHCP konfiguriert war, sendete der LANCOM DHCP-Client ARP requests, obwohl diese für die WWAN-Verbindung nicht benötigt wurden.
- Die in dem Menü ‚IPv4 / Adressen‘ hinterlegten DNS-Server sind an das LAN-Interface gebunden. Wenn in diesem Menü die lokale IP-Adresse des Routers als DNS-Server hinterlegt und eine Default-Route erstellt wurde, welche auf die IP-Adresse eines vorgeschalteten Routers im selben IP-Adress-Bereich zeigte, führte dies zu einem unvermittelten Neustart des Routers.

**WLAN**

- Wenn bei voll ausgefüllter RADIUS-Benutzertabelle ein weiterer Benutzer hinzugefügt werden sollte, wurde anstatt einer Fehlermeldung eine Seite mit JavaScript-Code angezeigt.
- In LCOS 10.70 konnte es vorkommen, dass in der Adress-Tabelle des verwendeten WLC-Tunnels ein fehlerhafter Verweis auf die MAC-Adresse des verbundenen WLAN-Gerätes hinterlegt wurde. Dadurch funktionierte die Kommunikation über den WLC-Tunnel nicht mehr.

## 7. Allgemeine Hinweise

### Haftungsausschluss

Die LANCOM Systems GmbH übernimmt keine Gewähr und Haftung für nicht von der LANCOM Systems GmbH entwickelte, hergestellte oder unter dem Namen der LANCOM Systems GmbH vertriebene Software, insbesondere nicht für Shareware und sonstige Fremdsoftware.

### Sichern der aktuellen Konfiguration

**Bitte sichern Sie vor dem Update Ihrer LANCOM-Geräte auf eine neue LCOS-Version unbedingt Ihre Konfigurationsdateien!**

Wegen umfangreicher Feature-Erweiterungen ist ohne eine Sicherung der Konfigurationsdaten eine Rückkehr auf die alte Firmware **nicht mehr automatisch möglich**.

Wenn Sie Geräte, die Sie über eine Router-Verbindung oder WLAN-Punkt-zu-Punkt-Verbindung erreichen können, aktualisieren möchten, bedenken Sie bitte, dass Sie zuerst das entfernte LANCOM Gerät und anschließend das lokale LANCOM Gerät aktualisieren. Eine Anleitung zur Firmware-Aktualisierung erhalten Sie im LCOS-Referenzhandbuch. **Wir empfehlen zudem, dass produktive Systeme vor dem Einsatz in der Kundenumgebung erst einem internen Test unterzogen werden**, da trotz intensivster interner und externer Qualitätssicherungsmaßnahmen ggf. nicht alle Risiken durch LANCOM Systems ausgeschlossen werden können.

### Verwendung einer Minimalfirmware zur Vergrößerung des Speicherplatzes

Durch zahlreiche neue Funktionen in der LCOS-Firmware ist es bei älteren LANCOM Geräten unter Umständen nicht mehr möglich, zwei vollwertige Firmware-Versionen gleichzeitig zu speichern. Um mehr Platz im Speicher zu schaffen, muss dann statt einer vollwertigen Firmware zunächst eine eingeschränkte, kleinere Firmware eingerichtet werden. Hierdurch steht für die andere Firmware im Gerät erheblich mehr Speicher zur Verfügung. Diese Einrichtung ist nur einmalig erforderlich und wird mit einer „Minimalfirmware“ durchgeführt. Nach dem Einspielen der Minimalfirmware steht die Firmsafe-Funktion des LANCOM nur noch in eingeschränktem Umfang zur Verfügung. Das Update auf eine neuere Firmware ist weiterhin problemlos möglich. Das LANCOM Gerät arbeitet nach einem fehlgeschlagenen Update jedoch mit einer Minimalfirmware, die Ihnen ausschließlich den lokalen Zugriff auf das Gerät erlaubt. Alle erweiterten Funktionalitäten, insbesondere die Remote Administration, sind nicht verfügbar, solange die Minimalfirmware aktiv ist.